# Lecture Notes in Computer Science 12819

More information about this subseries at http://www.springer.com/series/7407

Antonio Cerone · Peter Csaba Ölveczky (Eds.)

# Theoretical Aspects of Computing – ICTAC 2021

18th International Colloquium
Virtual Event, Nur-Sultan, Kazakhstan, September 8–10, 2021
Proceedings

Springer

*Editors*
Antonio Cerone
Nazarbayev University
Nur-Sultan, Kazakhstan

Peter Csaba Ölveczky
Department of Informatics
University of Oslo
Oslo, Norway

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-85314-3 ISBN 978-3-030-85315-0 (eBook)
https://doi.org/10.1007/978-3-030-85315-0

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues



This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

This volume contains the proceedings of the 18th International Colloquium on Theoretical Aspects of Computing (ICTAC 2021), which was held during September 8–10, 2021. The event was supposed to take place in Nur-Sultan, Kazakhstan, but due to the pandemic it had to be held as a fully virtual event, organized by Nazarbayev University.

The conference concerns all aspects of theoretical computer science and aims at bringing together researchers and practitioners from academia, industry, and government to present research and exchange ideas and experience, addressing challenges in both theoretical aspects of computing and the exploitation of theory through methods and tools for system development. ICTAC also aims to promote research cooperation between developing and industrial countries.

ICTAC 2021 received 55 paper submissions. Almost all papers received at least three reviews. Based on the reviews and extensive discussions, the program committee decided to accept 20 papers. This volume contains the revised versions of these 20 papers, which cover a wide variety of topics, including: getting the best price for selling your personal data; attacking Bitcoin; optimizing various forms of model checking; synthesizing and learning algorithms; formalizing and verifying contracts, languages, and compilers; analyzing the correctness and complexity of programs and distributed systems; and finding connections from proofs in propositional logic to quantum programming languages.

The conference also featured invited talks by Wil van der Aalst (RWTH Aachen University, Germany), Alan Dix (Swansea University, UK), Kim Guldstrand Larsen (Aalborg University, Denmark), and Grigore Rosu (University of Illinois at Urbana-Champaign, USA). An abstract of the invited talk by Larsen and full papers accompanying those by van der Aalst and Dix are included in this volume.

Many colleagues and friends contributed to ICTAC 2021. We thank the invited speakers for accepting our invitations to give invited talks and the authors who submitted their work to ICTAC 2021. We are grateful to the members of the program committee and the external reviewers for providing timely and insightful reviews, as well as for their involvement in the post-reviewing discussions. We would also like to thank the regional publicity chairs for their work attracting submissions and Springer for sponsoring the Best Paper Award.

July 2021

Antonio Cerone
Peter Csaba Ölveczky

# Organization

## Program Chairs

| | |
|---|---|
| Antonio Cerone | Nazarbayev University, Kazakhstan |
| Peter Csaba Ölveczky | University of Oslo, Norway |

## Steering Committee

| | |
|---|---|
| Frank de Boer | CWI, The Netherlands |
| Martin Leucker (Chair) | University of Lübeck, Germany |
| Zhiming Liu | Southwest University, China |
| Tobias Nipkow | Technical University of Munich, Germany |
| Augusto Sampaio | Federal University of Pernambuco, Brazil |
| Natarajan Shankar | SRI International, USA |
| Tarmo Uustalu | Tallinn University of Technology, Estonia |

## Program Committee

| | |
|---|---|
| Erika Ábrahám | RWTH Aachen University, Germany |
| Bernhard K. Aichernig | Graz University of Technology, Austria |
| Musab A. Alturki | Runtime Verification Inc., USA, and King Fahd University of Petroleum and Minerals, Saudi Arabia |
| Étienne André | Université de Lorraine, France |
| Ebru Aydin Gol | Middle East Technical University, Turkey |
| Kyungmin Bae | Pohang University of Science and Technology, South Korea |
| Maurice ter Beek | ISTI-CNR, Italy |
| Dirk Beyer | Ludwig-Maximilian University Munich, Germany |
| Simon Bliudze | Inria Lille, France |
| Roberto Bruni | University of Pisa, Italy |
| Antonio Cerone | Nazarbayev University, Kazakhstan |
| Manuel Clavel | Vietnamese-German University, Vietnam |
| Adrian Francalanza | University of Malta, Malta |
| Rob van Glabbeek | Data61, CSIRO, Australia |
| Sergey Goncharov | Friedrich-Alexander University Erlangen-Nürnberg, Germany |
| Jan Friso Groote | Eindhoven University of Technology, The Netherlands |
| Stefan Gruner | University of Pretoria, South Africa |
| Osman Hasan | National University of Sciences & Technology, Pakistan |
| Klaus Havelund | Jet Propulsion Laboratory, USA |
| Kim G. Larsen | Aalborg University, Denmark |

| | |
|---|---|
| Axel Legay | Université catholique de Louvain, Belgium |
| Martin Leucker | University of Lübeck, Germany |
| Manuel Mazzara | Innopolis University, Russia |
| Catherine Meadows | Naval Research Laboratory, USA |
| Larissa Meinicke | The University of Queensland, Australia |
| Hans de Nivelle | Nazarbayev University, Kazakhstan |
| Kazuhiro Ogata | JAIST, Japan |
| Peter Csaba Ölveczky | University of Oslo, Norway |
| Catuscia Palamidessi | Inria, France |
| Elaine Pimentel | Federal University of Rio Grande do Norte, Brazil |
| José Proença | Polytechnic Institute of Porto, Portugal |
| Riadh Robbana | INSAT, Carthage University, Tunisia |
| Gwen Salaün | University of Grenoble Alpes, France |
| Davide Sangiorgi | University of Bologna, Italy, and Inria, France |
| Lutz Schröder | Friedrich-Alexander University Erlangen-Nürnberg, Germany |
| Volker Stolz | Western Norway University of Applied Sciences, Norway |
| Georg Struth | The University of Sheffield, UK |

## Regional Publicity Chairs

| | |
|---|---|
| Stefan Gruner | University of Pretoria, South Africa |
| Kazuhiro Ogata | JAIST, Japan |
| Elaine Pimentel | Federal University of Rio Grande do Norte, Brazil |
| Riadh Robbana | INSAT, Carthage University, Tunisia |
| Nikolay Shilov | Innopolis University, Russia |

## Additional Reviewers

Yehia Abd Alrahman
Mario S. Alvim
Tomer Ashur
Giorgio Bacci
Marco Bernardo
Laura Bussi
Guillermina Cledou
Khanh Huu The Dam
Guillaume Dupont
Rick Erkens
Lorenzo Gheri
Imen Ben Hafaiedh
Andreas Hülsing
Peter Gjöl Jensen
Karam Kharraz
Michalis Kokologiannakis
Sandeep Kulkarni
Frédéric Lang
Thomas Lemberger
Anders Miltner
Carlos Olarte
Renato Neves
Andrea Pferscher
Johannes Åman Pohjola
Danny Bøgsted Poulsen
Adnan Rashid
Jose Ignacio Requeno
Martin Sachenbacher

Wendelin Serwe
Francesco Sica
Flip van Spaendonck
Daniel Thoma
Adele Veschetti
Olivier Verdier
Nico Weise

## Sponsor

NAZARBAYEV
UNIVERSITY

# Model Checking and Machine Learning Joining Forces in UPPAAL (Invited Paper)

Kim Guldstrand Larsen

Department of Computer Science, Aalborg University, Denmark

In the talk we offer a detailed presentation on how the symbolic model checking techniques of Uppaal has joined forces with machine learning during the last 10 years.

The first step towards exploiting the efficiency of machine learning in UPPAAL was made in the branch UPPAAL SMC. Here [5], UPPAAL SMC offers highly efficient statistical model checking capabilities in order to provide performance analysis for a rich class of stochastic hybrid automata [10], and in a manner that consistently refines the Boolean verdicts of the model checking capability of classical UPPAAL. During the last 10 years this effort includes development of a sound theoretical foundation (e.g. the underlying stochastic semantics of timed automata [2]), the supporting algorithmic analysis (e.g. sequential testing a'la Wald), the efficient tool implementation as well as a long range of applications.

Most recently the SMC engine of UPPAAL has been considerably accelerated by exploiting independencies of system components during generation of random runs. In UPPAAL SMC , as in Gillespie's algorithm for biochemical systems, components are repeatedly racing against each other, calling for a resampling of all components after each step. A challenge is to prove that resampling only step-dependent components leave the probability distribution on runs unchanged. Another challenge is to develop static analysis methods for identifying independencies. This in turn has significantly reduced the complexity of run-generation (from quadratic to – in practice – linear), allowing UPPAAL SMC to scale to millions of components, as witnessed by recent applications to so-called Agent-based models for COVID19 analysis with millions of components, e.g. one per citizen of Denmark [9]. In addition, using the SMC engine may be used to generate synthetic data from stochastic hybrid automata in order to learn Bayesian networks for infering beliefs of key observable and unobservable properties in settings with scares data [8].

In the most recent branch UPPAAL STRATEGO [4, 3], symbolic techniques are combined with reinforcement learning to efficiently obtain near-optimal yet safe strategies for hybrid Markov decision processes. Taking as inputs 1) a hybrid Markov decision process $H$, 2) a safe constraint $\phi$ and 3) an objective function $O$ to be optimized, UPPAAL STRATEGO first provides a most permissive safety strategy guaranteeing that $\phi$ is fullfilled using a timed game abstraction of $H$. Here well-known symbolic model checking techniques are used. Next, applying various learning methods, sub-strategies (thus still safe) optimizing O are subsequently obtained. The talk will present new (Q-, M-, ..) learning methods developed [7], preliminary results on their convergence [6], the ability to learn and output small and explainable strategies using decision trees

[1], and the approach for taking partial observability into account. In addition the talk will provide a demonstration of the new UPPAAL STRATEGO on the Smart Farming Challenge of the Dagstuhl seminar "Analysis of Autonomous Mobile Collectives in Complex Physical Environments" (October 2019). Also on-going applications of UPPAAL STRATEGO on water-management, traffic-light control, energy-aware building ao will be pointed out.

During the next five-year period the effort on combining model checking and machine learning will continue in the newly granted Villum-Investigator Center S4OS[1] of the speaker.

## References


1. Ashok, P., Křetínský, J., Larsen, K. G., Le Coënt, A., Taankvist, J. H., Weininger, M.: SOS: Safe, optimal and small strategies for hybrid markov decision processes. In: Parker, D., Wolf, V. (eds.) Quantitative Evaluation of Systems. QEST 2019. LNCS, vol. 11785, pp. 147–164 Springer, Cham (2019). https://doi.org/10.1007/978-3-030-30281-8_9
2. Bertrand, N., et al.: Stochastic timed automata. Log. Methods Comput. Sci., **10**(4), 2014
3. David, A., et al.: On time with minimal expected cost!. In: Cassez, F., Raskin, J. F. (eds.) Automated Technology for Verification and Analysis. ATVA 2014. LNCS, vol. 8837, pp. 129–145. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-11936-6_10
4. David, A., Jensen, P. G., Larsen, K. G., Mikučionis, M., Taankvist, J. H.: UPPAAL STRATEGO. In: Baier, C., Tinelli, C. (eds.) Tools and Algorithms for the Construction and Analysis of Systems. TACAS 2015. LNCS, vol. 9035, pp. 206-211. Springer, Berlin, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46681-0_16
5. David, A., Larsen, K. G., Legay, A., Mikucionis, M., Poulsen, D. B.: UPPAAL SMC tutorial. Int. J. Softw. Tools Technol. Transf. **17**(4), 397–415 (2015)
6. Jaeger, M., Bacci, G., Bacci, G., Larsen, K. G., Jensen, P. G.: Approximating euclidean by imprecise markov decision processes. In: Margaria, T., Steffen, B. (eds.) Leveraging Applications of Formal Methods, Verification and Validation: Verification Principles. ISoLA 2020. LNCS, vol. 12476, pp. 275–289. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-61362-4_15
7. Jaeger, M., Jensen, P. G., Guldstrand L. K., Legay, A., Sedwards, S., Taankvist, J. H.: Teaching stratego to play ball: optimal synthesis for continuous space MDPs. In: Chen, Y.F., Cheng, C. H., Esparza, J. (eds.) Automated Technology for Verification and Analysis. ATVA 2019. LNCS, vol. 11781, pp. 81–97. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-31784-3_5
8. Jaeger, M., Larsen, K. G., Tibo, A.: From statistical model checking to run-time monitoring using a bayesian network approach. In: Deshmukh, J., Ničković, D. (eds.) Runtime Verification. RV 2020. LNCS, vol. 12399, pp. 517–535. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-60508-7_30


[1] S4OS: Scalable analysis and Synthesis of Safe, Small, Secure and Optimal Strategies for CPS.

9. Jensen, P. G., Jørgensen, K. Y., Larsen, K. G., Mikučionis, M., Muñiz, M., Poulsen, D. B.: Fluid Model-Checking in Uppaal for Covid-19. In: Margaria, T., Steffen, B. (eds.) Leveraging Applications of Formal Methods, Verification and Validation: Verification Principles. ISoLA 2020. LNCS, vol. 12476, pp. 385–403. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-61362-4_22
10. Larsen, K. G.: Statistical model checking, refinement checking, optimization, … for stochastic hybrid systems. In: Jurdziński, M., Ničković, D. (eds.) Formal Modeling and Analysis of Timed Systems. FORMATS 2012. LNCS, vol. 7595, pp. 7–10. Springer, Berlin, Heidelberg (2012). https://doi.org/10.1007/978-3-642-33365-1_2

# Contents

## Quantum Computing



## Security and Privacy



## Synthesis and Learning



## Systems Calculi and Analysis